(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01271 A1

(51) International Patent Classification[7]: G02B 21/00, 21/16

(21) International Application Number: PCT/EP01/07090

(22) Internaational Filing Date: 22 June 2001 (22.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/606,339 29 June 2000 (29.06.2000) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: KRASINSKI, Raymond; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). ROSNER, Martin; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: HOEKSTRA, Jelle; Internationaal Octrooibureau B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

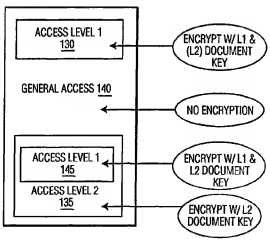
(81) Designated States (national): CN, JP, KR.

(84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— with international search report
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: MULTIPLE ENCRYPTION OF A SINGLE DOCUMENT PROVIDING MULTIPLE LEVEL ACCESS PRIVILEGES



(57) Abstract: A method and system for selectively encrypting and decrypting different sections of a document provides different access levels in a technique employing different keys. The documents may be encrypted at a document section level ("section" here used according to its general meaning) and uses a different set of encryption keys for each section. A user A with an access level 1 may access only those section encoded with access level 1 plus unencoded sections. An application example of this technique is in hospitals. A patients records may each be segmented into separately-encrypted portions giving access to nurses for only suitable material while giving broader access to doctors. The nurse would be provided with his/her access level private key to gain access to those parts of the document for which nurses have rights. There could also be a level to which only the primary care physician or health care proxy has access.

WO 02/01271 A1

Multiple encryption of a single document providing multiple level access privileges

5

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The invention relates to document encryption and access restrictions on documents and more particularly to the encryption of each portion of a document such that
10 access rights to respective portions may be obtained with corresponding keys.

BACKGROUND

Various kinds of document access protection are known. In one example, EP 0 848 314 A1 for DOCUMENT SECURITY SYSTEM AND METHOD only documents to which the user has rights are generated from a database. Varying security levels are
15 provided. Another system described in US Patent No. 5,052,040 for MULTIPLE USER STORED DATA CRYPTOGRAPHIC LABELING SYSTEM AND METHOD permits different users to utilize the same files. The system exploits an extension of the file label which contains configuration capabilities and user rights and privileges. The separate user rights and privileges in this case relate to the entire document such as read only, read and
20 write, deletion, etc. The document is encrypted. Another prior art system is described in US Patent No. 6,011,847 for CRYPTOGRAPHIC ACCESS AND LABELING SYSTEM. In this system, encryption and decryption of files uses a relational key generated by the system. A computer program also generates a series of labels that are encrypted and appended as a trailer to the encrypted message. The encrypted labels provide a history behind the particular
25 encryption and they can be individually selected, separated, and decrypted from the total file. An access control module provides access to an encryption portion of the document to users with passphrases by comparing a generated vector or key with a partially decrypted version of a second vector or key stored on a portable storage medium such as a floppy disk. In response, a main key can be generated to encrypt or decrypt the labels. The latter system is
30 mainly concerned with adding descriptive labels to the end of an encrypted document and contains a key exchange method for passing the decryption key between a server and a client.

Other prior art systems and methods are known, but none contain a very convenient, robust, and straightforward method for encryption-protection of different parts of a document based on access privileges.

SUMMARY OF THE INVENTION

A method and system for selectively encrypting and decrypting different sections of a document provides different access levels in a technique employing different keys. The documents may be encrypted at a document section level ("section" here used according to its general meaning) and uses a different set of encryption keys for each section. A user A with an access level 1 may access only those sections encoded with access level 1 plus unencoded sections. An application example of this technique is in hospitals. A patients records may each be segmented into separately-encrypted portions giving access to nurses for only suitable material while giving broader access to doctors. Thus, this example illustrates access control to information contained inside a document based on pre-defined roles accepted within a specific environment. The nurse would be provided with an access level key based on the access control rules defined by the hospital. Such key would allow the nurse to gain access to those parts of the document for which nurses have rights. There could also be a level to which only the primary care physician or health care proxy has access.

A method for distributing keys is also provided. This method utilizes a key box which is created for holding keys used to encode the sections of the document. The key box contains a slot for each level of access. The set of keys that a user at a given level requires is placed in a corresponding slot. Each slot is encoded using the access level public key giving the user access to the keys in the appropriate slot when decrypted using the user's private key.

An additional feature provides an outer layer of encryption using a public key for a requesting organization. Once the requesting organization opens the document using its private key, anyone in the receiving organization can apply their access level private key(s) to the key box, which in turn applies the keys in the corresponding slot to the document. This allows each user to view/modify the parts of the document to which they have access rights.

The invention will be described in connection with certain preferred embodiments, with reference to the following illustrative figures so that it may be more fully understood. The description of this invention uses the definition of public key to correspond to the public portion of the public/private key pair that is used in the art to realize asymmetric algorithms. The description of this invention uses the definition of private key to correspond to the private portion of the public/private key pair that is used in the art to realize asymmetric algorithms. The description of this invention uses the definition of symmetric key to refer to the a single key that is used in the art to realize symmetric algorithms.

With reference to the figures, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of the preferred embodiments of the present invention only, and are presented in the cause of providing what is believed to be the most useful and readily understood description of the principles and conceptual aspects of the invention. In this regard, no attempt is made to show structural details of the invention in more detail than is necessary for a fundamental understanding of the invention, the description taken with the drawings making apparent to those skilled in the art how the several forms of the invention may be embodied in practice.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is an illustration of a computer environment in which the invention may be used.

Fig. 2A is an illustration of a document indicating separate sections and the encryption processes to be applied to each section according to first embodiment of the invention in which public keys are used for encryption.

Fig. 2B is an illustration of a document indicating separate sections and the encryption processes to be applied to each section according to second embodiment of the invention in which public keys are used for encryption.

Fig. 3 is an illustration of a document indicating separate sections and the encryption processes to be applied to each section according to third embodiment of the invention in which document-specific keys are used.

Fig. 4 is an illustration of a key box document used with the embodiment of Fig. 3.

Fig. 5 is an illustration of a process for encrypting a document according to an embodiment compatible with any of the foregoing embodiments.

Fig. 6 is an illustration of a process for encrypting a document according to an embodiment compatible with any of the foregoing embodiments.

Fig. 7 is an alternative way of packaging the key box in a transmission by including it within a single document.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to Fig. 1, the invention may be used in the environment of electronic document transfer. An example of such an environment is a sending computer 110 and a

receiving computer 120 connected by a network 100 or simply by physical transfer of a non-volatile data store 90 such as a floppy disk.

Referring to Fig. 2A, a document 95 contains various sections 130, 135, 140, and 145. Each section is divided according to how the information contained in the section is desired to be made available to a particular person (organization or other entity) or class of persons. The document 95 is intended to be transferred by the sender 110 to the receiver 120, the receiver including each of the persons or classes of persons. The sections labeled 130 and 145 are encrypted with a public key L1 corresponding to the first user or class of users. The section labeled 135 is encrypted with a second public key L2 corresponding to the second user or class of users. By virtue of being embedded in the section 135, section 145 is also encrypted with the L2 public key.

Referring to Fig. 2B, the various sections may be encrypted with only one key or all keys from the access level to which they correspond down to the lowest level of access. Thus, in this example, document section 145 is encrypted with both the L1 and L2 keys, but so is document section 130. Alternatively, each section may be encrypted with only a single key, so that a level 1 section appearing in a level 2 section is simply treated as a completely separate section with the level 2 section being broken into separate subsections for L2 encryption. The encryption methods described above permit multilevel access to a document based on the public keys of the intended audience. It is possible to limit access based on the user as well as the particular document as shown in the next embodiment.

Referring now to Figs. 3 and 4, the document sections are encrypted with respective document keys, a respective one for each access level defined within the scope of the document. The document keys may be symmetric keys. The latter are not shared outside of the context of use of the document and the user need never directly know what the symmetric keys are. These document keys are then made available to the recipients by encrypting them into a separate document (which could be part of the original document as in a file header as illustrated in Fig. 7) called a key box. The key box has a slot corresponding to each access level defined within the scope of the organization that is requesting such document. A first slot 1 210 contains document keys for access levels 1 and 2 giving the user access to both levels. A second slot 1 215 contains document keys for access level 2. Each slot is encrypted using the public key of the organization that corresponds to the access level of the slot. The entire key box file and the document may be encrypted using the public key of the user to ensure confidentiality of the transmission of the document and the key box.

Additionally, the key box and the document may be signed by the sender 110 to ensure integrity of the transmission and authenticity of the document.

The preceding embodiment contemplates an agreement between the sender of the document who prepares the encryption and the organization receiving the document. This agreement would map access levels used in encrypting the document to the access levels in place at the receiver. For a given document, a given organization level may map to a single document access level. Alternatively, a given organization level may map to multiple document access level.

Preferably, to assure data integrity and non-repudiation, the document source may sign the document hash with a private key. The requestor receiving the document together with the signature can then vouch for the validity of the source. Other mechanisms for authenticating the document's contents may also be used.

When a person with access level N opens the document, he/she presents his/her organization access level private key, which corresponds to the asymmetric key pair, to a decryption process that uses the key to access the appropriate slot in the key box. The symmetric keys may be used by the process to access the appropriate levels of the document transparently to the user. The user never "handles" the symmetric document keys and simply accesses the portions of the document the user has permission to access.

Referring now to Fig. 5, the detailed steps for creating, sending, receiving, and using a document begin with the receipt of a request S10 for the document and the appropriate information such as the public keys of the users, a map of users to access levels, etc. Next, a key is created for each access level required S20. The document is then encrypted starting with the highest (most privileged) access level and going down S30. This may result in the layered encryption of either of Figs. 2A and 2B or the alternative process where each level is only encrypted once. The keys are formed into a key box document and each set separately encrypted using the public keys of the access levels S45. Then the document and key box are bundled and optionally encrypted using the public key of the receiver S55.

When the receiver receives the file containing the encrypted document and the key box, the package is unbundled and optionally decrypted S60. The document and key box are then made available to the users S70. When a user accesses the document, the user provides his/her organization access level private key to a decryption process on a receiving computer (e.g. 120) which uses the key to decrypt the appropriate slot of the key box S75. The process then applies the symmetric keys, obtained from the decrypted slot in the key

box, S80 to the document to allow the user to access the document S85. The user never directly accesses the symmetric access level keys or even concerns him/herself with how many keys are involved.

Referring to Fig. 6, in an alternative embodiment, the public keys of the receivers are not used to encrypt the document. Rather step S45 is skipped and the key box is simply encrypted using the organization's public key. At the receiving organization, an additional step S90 between S65 and S70 is added wherein the slots of the key box are mapped to the access levels present in the organization and encrypted with the appropriate public keys of the users or group of users.

It will be evident to those skilled in the art that the invention is not limited to the details of the foregoing illustrative embodiments, and that the present invention may be embodied in other specific forms without departing from the spirit or essential attributes thereof. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than by the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

CLAIMS:

1. A method of securely transmitting a first document, comprising the steps of:

- generating first and second level document keys;
- encrypting a first section (130) of said first document with said first level document key and encrypting said first and a second section (135) of said first document with said second level document key;
- forming a second document (220) or a portion (520) of said document, said second document or said portion containing said first and second level document keys;
- transmitting said first document or said first and second documents as appropriate to the choice in said step of forming.

2. A method as in claim 1, wherein said first and second level document keys are symmetric keys.

3. A method as in claim 1, further comprising receiving at least two public keys from a recipient, said step of forming including encrypting said second document such that a corresponding set of said first and second level document keys is made available by decryption using a first of said at least two public keys and such that a corresponding other set of said first and second level document keys is made available by decryption using said second of said at least two public keys.

4. A method as in claim 3, wherein said step of encrypting including encrypting a first of said at least two public keys in a first portion of said second document or first document portion and encrypting a first and second of said at least two public keys in a second portion of second document or first document portion.

5. A method as in claim 3, wherein said first and second level document keys are symmetric keys.

6. A method as in claim 1, wherein said step of transmitting includes encrypting said first document or said first and second documents as appropriate to the choice in said step of forming.

7. A method of encrypting a document, comprising the steps of:

- encrypting a first portion of a document using a first key;
- encrypting a second portion of said document using a second key;
- encrypting a result of said first and second steps of encrypting using a third key, being a public key of a recipient.

8. A method of encrypting a document as in claim 7,wherein said first key is a first public key of said recipient and said second key is a second public key of said recipient.

9. A method of encrypting a document as in claim 7, wherein said first key is a first symmetric key and said second key is a second symmetric key, and the method includes the step of encrypting said first symmetric key with a public key.

10. A method as in claim 9, wherein said second portion includes a part of said first portion, said part having been encrypted with said first symmetric key.

11. A method of encrypting a document as in claim 9, comprising the step of encrypting said second symmetric key with a second public key.

12. A method of securely providing access to first and second readers of a document, comprising the steps of:

- transmitting to a sender of a document, public keys corresponding to readers of said document, said public keys being used to encrypt said document;
- receiving encrypted data from said sender;

decrypting a portion of said encrypted data using a private key corresponding to one of said public keys;

- a result of said first step decrypting being the accessing of a portion of said data corresponding to said one of said public keys;
- decrypting a portion of said encrypted data using a private key corresponding to another of said public keys;

- result of said second step decrypting being the accessing of a portion of said data corresponding to said other of said public keys.

13. A method as in claim 12, wherein said first and second steps of decrypting each include decrypting a portion of said data to unlock a respective set of encryption keys.

14. A method as in claim 12, wherein said first and second steps of decrypting further include using said respective set of encryption keys to unlock at least a portion of said encrypted data to provide access to only a portion of said document.

15. A method as in claim 12, wherein said first and second steps of decrypting further include using said respective set of encryption keys to unlock at least a portion of said encrypted data to provide access to said document.

16. A data file (95+220), comprising:
an encryption protected document (95, 595) containing a key portion (520) and an encrypted document portion (585);
- said key portion being at least partly decryptable with a first public key to provide access to a first symmetric key;
- said key portion being at least partly decryptable with a second public key to provide access to a second symmetric key;
- a first portion (210) of said encrypted document portion being decryptable with said first symmetric key and a second portion (215) of said encrypted document portion being decryptable with said second symmetric key.

17. A data file containing:
- an encrypted document (95) and at least two encryption keys;
- said encryption keys being encrypted such as to be accessible using at least two public keys and such that a first portion (130) of said encrypted document is accessible by decrypting with a first subset of said encryption keys, said first subset being decryptable using a first of said at least two public keys, and such that a second portion of said encrypted document is accessible by decrypting with a second subset of said encryption keys, said second subset being decryptable using a second of said at least two public keys.

18. A data set stored on a data storage medium, comprising:

- a document encrypted in portions using respective keys to encrypt said portions;
- a first portion of said document being encrypted with a first of said respective keys;
- a second portion of said document being encrypted with a second of said respective key;
- said first and second respective keys being encrypted in a file such as to permit decryption of said first key by a first private key and to permit decryption of said second key by a second private key.

19. A data set stored on a data storage medium, comprising:

- document encrypted in portions using respective keys to encrypt said portions;
- a first portion of said document being encrypted with first and second of said respective keys;
- a second portion of said document being encrypted with said first respective key;
- said first and second respective keys being encrypted in a file such as to permit decryption of said first and second keys by a first private key and to permit decryption of said first key by a second private key.

20. A document decrypting program stored on a data storage medium, comprising:

- code defining a process capable of selectively decrypting a portion of a data set using a respective key, said portion yielding a respective set of further keys upon decryption;
- code defining a further process capable of retrieving from said data set portions of a document corresponding to said respective set of further keys to provide access to only portions of said document corresponding to respective key.

21. A stored program as in claim 20, wherein said respective key is a public key.

22. A stored program as in claim 20, wherein each of said set of further keys is unique to said document.

23. A stored program as in claim 20, wherein each of said set of further keys is a symmetric key.

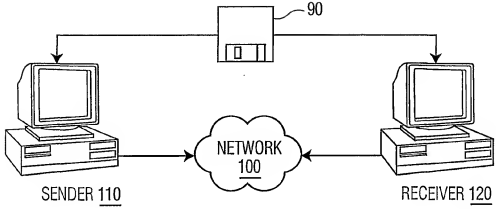

90
NETWORK
100
SENDER 110
RECEIVER 120

FIG. 1

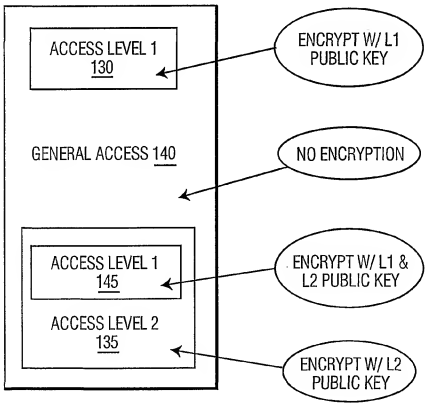

ACCESS LEVEL 1
130
ENCRYPT W/ L1
PUBLIC KEY
GENERAL ACCESS 140
NO ENCRYPTION
ACCESS LEVEL 1
145
ENCRYPT W/ L1 &
L2 PUBLIC KEY
ACCESS LEVEL 2
135
ENCRYPT W/ L2
PUBLIC KEY

FIG. 2A

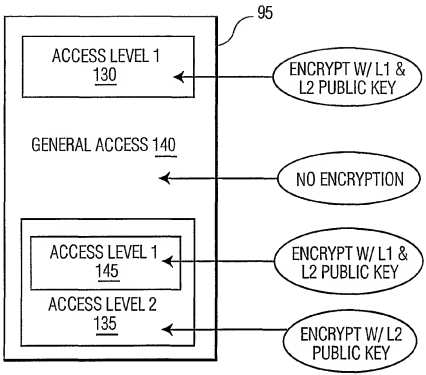

95
ACCESS LEVEL 1
130
ENCRYPT W/ L1 &
L2 PUBLIC KEY
GENERAL ACCESS 140
NO ENCRYPTION
ACCESS LEVEL 1
145
ENCRYPT W/ L1 &
L2 PUBLIC KEY
ACCESS LEVEL 2
135
ENCRYPT W/ L2
PUBLIC KEY

FIG. 2B

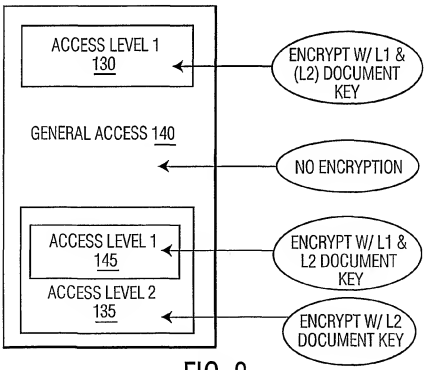

ACCESS LEVEL 1
130
ENCRYPT W/ L1 &
(L2) DOCUMENT
KEY
GENERAL ACCESS 140
NO ENCRYPTION
ACCESS LEVEL 1
145
ENCRYPT W/ L1 &
L2 DOCUMENT
KEY
ACCESS LEVEL 2
135
ENCRYPT W/ L2
DOCUMENT KEY

FIG. 3

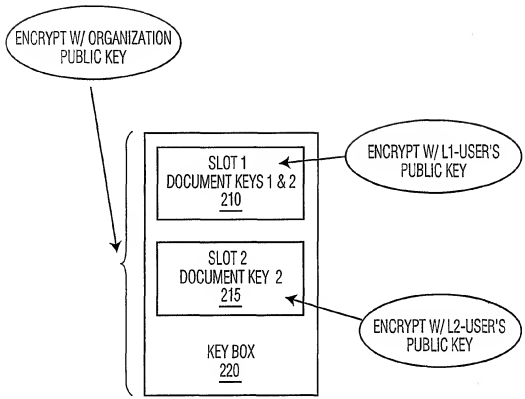

ENCRYPT W/ ORGANIZATION PUBLIC KEY
SLOT 1
DOCUMENT KEYS 1 & 2
210
ENCRYPT W/ L1-USER'S PUBLIC KEY
SLOT 2
DOCUMENT KEY 2
215
ENCRYPT W/ L2-USER'S PUBLIC KEY
KEY BOX
220

FIG. 4

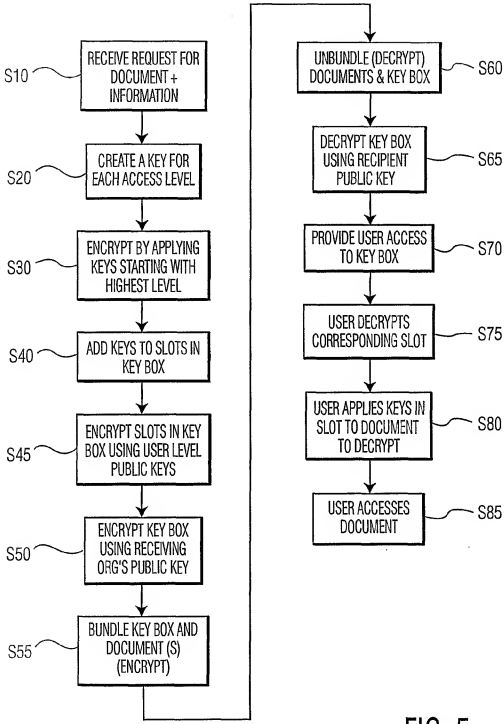

S10
RECEIVE REQUEST FOR DOCUMENT + INFORMATION
S20
CREATE A KEY FOR EACH ACCESS LEVEL
S30
ENCRYPT BY APPLYING KEYS STARTING WITH HIGHEST LEVEL
S40
ADD KEYS TO SLOTS IN KEY BOX
S45
ENCRYPT SLOTS IN KEY BOX USING USER LEVEL PUBLIC KEYS
S50
ENCRYPT KEY BOX USING RECEIVING ORG'S PUBLIC KEY
S55
BUNDLE KEY BOX AND DOCUMENT (S) (ENCRYPT)
S60
UNBUNDLE (DECRYPT) DOCUMENTS & KEY BOX
S65
DECRYPT KEY BOX USING RECIPIENT PUBLIC KEY
S70
PROVIDE USER ACCESS TO KEY BOX
S75
USER DECRYPTS CORRESPONDING SLOT
S80
USER APPLIES KEYS IN SLOT TO DOCUMENT TO DECRYPT
S85
USER ACCESSES DOCUMENT

FIG. 5

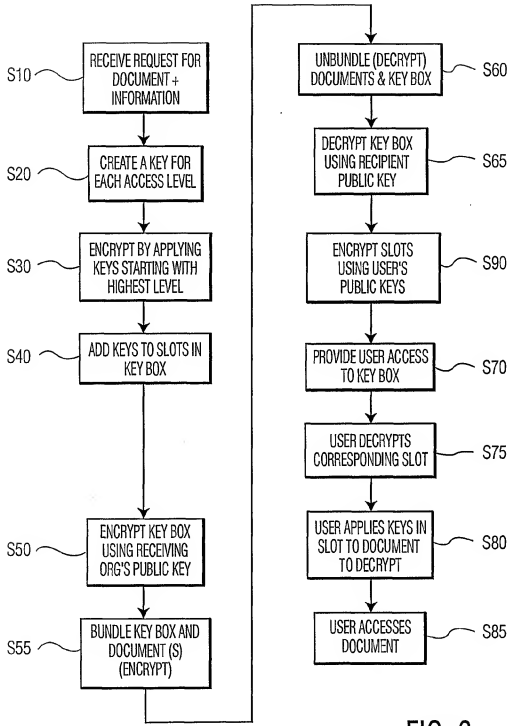

S10
RECEIVE REQUEST FOR DOCUMENT + INFORMATION
S20
CREATE A KEY FOR EACH ACCESS LEVEL
S30
ENCRYPT BY APPLYING KEYS STARTING WITH HIGHEST LEVEL
S40
ADD KEYS TO SLOTS IN KEY BOX
S50
ENCRYPT KEY BOX USING RECEIVING ORG'S PUBLIC KEY
S55
BUNDLE KEY BOX AND DOCUMENT (S) (ENCRYPT)
S60
UNBUNDLE (DECRYPT) DOCUMENTS & KEY BOX
S65
DECRYPT KEY BOX USING RECIPIENT PUBLIC KEY
S90
ENCRYPT SLOTS USING USER'S PUBLIC KEYS
S70
PROVIDE USER ACCESS TO KEY BOX
S75
USER DECRYPTS CORRESPONDING SLOT
S80
USER APPLIES KEYS IN SLOT TO DOCUMENT TO DECRYPT
S85
USER ACCESSES DOCUMENT

FIG. 6

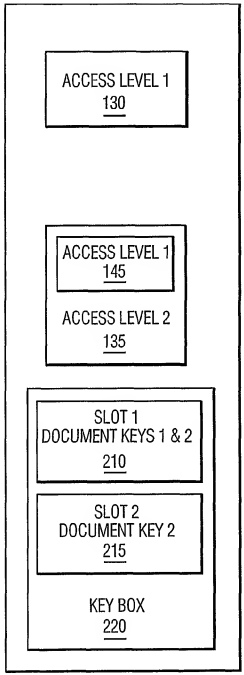

ACCESS LEVEL 1
130
ACCESS LEVEL 1
145
ACCESS LEVEL 2
135
SLOT 1
DOCUMENT KEYS 1 & 2
210
SLOT 2
DOCUMENT KEY 2
215
KEY BOX
220

FIG. 7